

REMARKS

Claims 1-21 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness

The examiner has rejected claims 1-21 under 35 U.S.C. § 103 as being unpatentable over Chang et al. (USPN 6105012) in view of Sasich et al. (USPN 6661904). This rejection is respectfully traversed.

In rejecting the claims, Examiner states in part:

As per claim 1, Chang teaches the invention substantially as claimed including the use of a data processing implemented method comprising: initiating a session, requesting a first web page, receiving the web page (col. 4 line 1-20...), encrypting the web page (col. 4 lines 20-22....)
Chang does not teach the use of securing information stored in a cache.

Sasich teaches the use of securing information stored in a cache (col. 7, lines 25-30, lines 46-55). It would have been obvious to one skilled in the art at the time of the invention to combine Chang and Sasich in order to have a secure cache. By having Sasich's secure cache system, a third party may not access information associated the cache (i.e., personal information).

Applicant respectfully submits that the teaching of Chang and Sasich are not properly combinable in the way proposed by Examiner, and that even if they were properly combinable, they still would not teach the present invention. Claim 1 is reproduced for purposes of discussion.

1. A data processing implemented method for securing information stored in a browser cache associated with a browser, the method comprising:
 - initiating a session;
 - requesting a first web page;
 - receiving the web page;
 - encrypting the web page; and
 - caching the web page.

Claim 1 is claimed in the context of "securing information stored in a browser cache associated with a browser...." Neither reference, Chang nor Sasich, addresses this issue. Because neither of the cited references are directed to the problem addressed by the present invention, their combination would not form the invention of claim 1, particularly in the context of a browser cache.

Chang is directed to a "security system and method for financial institution server and client web browser." The invention deals with using HTML format to send and receive, between a financial institution server and a client computer with a web browser, forms representing financial transactions. (See Abstract, lines 1-10). According to Chang, these forms are encrypted for transit. Though Chang is clearly concerned with security, Chang does not appear to teach or suggest the idea of encrypting the data to be cached for the purpose of keeping the data secure within the cache. Chang appears to be concerned with keeping the data secure during transmission where it is most vulnerable to interception by a hacker, and does not address desirability of protecting received pages at the browser.

To cure this deficiency, Examiner points to Sasich, stating that "Sasich teaches the use of securing information stored in a cache...." Examiner cites Sasich at col. 7, lines 25-30 and lines 46-55. These sections are reproduced below.

In step 108a, the personal data is deposited in a raw data cache which includes groupings of user specified personal and privacy data and transaction related protocols. Custom data caches may be formed in connection with certain kinds of transactions.

Each raw data cache will be encoded to operate at a designated level of security commensurate with protection appropriate to the kind of data contained within it and required by the anticipated transaction. Raw data cache level 1 may contain basic usernames, email address, and appropriate base level security. Raw data cache level 4 may contain credit card numbers and other sensitive personal financial data requiring higher designated levels of security and verification.

Though the above citations mention encoding the "raw data caches," Sasich does not teach this in the context of a browser program, as claimed in claim 1 of the present invention. Instead, Sasich is directed to a method of encoding data in an image ("personal

logo") for transmission. The above passages do not describe general treatment of data in Sasich, but only describe one step in the creation of the personal logo, which is then used to transmit the sensitive data. For example, Sasich states at col. 3, lines 1-5:

The present invention makes use of digital graphical bitmaps to establish a visual representation of a sender's identity and authority. Corresponding data streams are used to transmit the sender's identity, authority, and data associated with the sender across a network.

As described in Sasich detailed description, the caching steps recited by Examiner are not in the context of a browser, and are only one step in the creation of the personal logo, which is a method of encrypting data for transmission. Sasich is not directed to protecting cached web pages by encrypting them and caching them, as claimed in claim 1.

Specifically, the passages recited above by Examiner are in the context of Figure 2 of Sasich. At col. 5, lines 46-48, Sasich starts the discussion of the process:

FIG. 2 shows a methodology for creating a personal logo. To make use of the personal logo capability, the user may first install client software on his or her computer.

[Emphasis added.]

Sasich goes on describing the method of FIG. 2. Step 108a, from which Examiner draws the above cited language, is given in Sasich as part of the logo creation process. This differs significantly from the present invention, which is directed to encrypting and caching web pages. In the logo creation process, according to Sasich in FIG. 2, the steps include receiving a base image (105); processing it to make the image unique (106); optimizing the image (107); receive data for encoding (108); cache the data (108a); combine the data with the image (109); store the UGPI (110); and display the personal logo (110).

The underlined steps are intended to highlight the fact that Sasich is not receiving, encrypting, and caching a web page as claimed. Instead, the step of caching is recited in the context of creating the personal logo, which is used as a means to transmit

information securely. Hence, Applicant respectfully submits that the cited language from col. 7 stating, "Each raw data cache will be encoded to operate at a designated level of security commensurate with protection appropriate to the kind of data contained within it..." does not teach the claimed limitations of, "receiving the web page; encrypting the web page; and caching the web page."

Hence, it is respectfully submitted that the combination of references does not teach the claimed invention. Teaching to encrypt cached data (such as that recited by Sasich: name, email address, phone number, etc.) for a specific process to create a personal security logo does not make obvious all uses of encrypted data, especially that taught in the context of claim 1.

Hence, Applicant respectfully submits that the two references, even if properly combined, do not teach or suggest the claimed invention.

Further, the cited references do not mention or suggest the modifications necessary to reach the claimed invention. In order for the two cited references to teach the claimed invention, significant modifications to their teaching would be necessary. For example, the encryption of cached data of Sasich would have to be modified to apply to a downloaded web page. Alternately, the teaching of Chang would have to be modified to include encryption of cached web pages, which is not taught nor suggested. The mere fact that the prior art could be readily modified to arrive at the claimed invention does not render the claimed invention obvious; the prior art must suggest the desirability of such a modification. *In re Ochiai*, 71 F.3d 1565, 1570, 37 U.S.P.Q.2d 1127, 1131 (Fed. Cir. 1996); *In re Gordon*, 733 F.2d 900, 903, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984). Merely stating that the modification would have been obvious to one of ordinary skill without identifying an incentive or motivation for making the proposed modification is insufficient to establish a *prima facie* case.

It is also respectfully submitted that neither Chang nor Sasich specifically addresses the problem of the present invention, namely, protecting cached data in a user's machine that might be accessible to others. For example, the present invention states at pages 3 and 4:

Even when the cache is physically located on the user's computer, the user cannot assume that the contents of the disk cache are safe from outside intrusion, much less secure if another user has access to the user's web browser. Anyone having access to the user's web browser cache could conceivably reconstruct a user's web searching activity and deduce the subject matter of the search.

Nothing in Sasich nor Chang addresses this problem. Hence, it is respectfully submitted that the combination of Sasich and Chang cannot be properly combined in the way suggested by Examiner. Hence, claim 1 is believed distinguished from the cited references. Likewise, the other independent claims discuss the innovations of the present application in the context of a browser, and are believed distinguished on the grounds applicable to claim 1, argued above. For these reasons, all independent claims are believed distinguished from the cited references.

Applicant also points out that several of the dependent claims are independently distinguishable from the cited references. For example, claim 6 states:

6. The method recited in claim 1, wherein one of the browser and the browser cache is password protected from unauthorized users.

No such teaching is found in either reference. Examiner cites Chang at col. 7, lines 45-55, which states:

The HTML forms emanating from the financial server can contain any combination of the above mentioned new fields in a FORM tag. Furthermore, the present invention can also accommodate a version of HTML that does not incorporate any of the new fields. Although the present invention has been described with reference to a particular syntax for the new field in the HTML FORM tag, it is not limited to this particular embodiment. Any other syntax can be used provided that it provides a similar function.

This passage does not teach or suggest the limitations of claim 6. Likewise, in the event Examiner has cited the wrong reference and intended to cite Sasich at this passage against claim 6, Applicant respectfully submits that lines 45-55 of column 7 of Sasich,

reproduced above, do not teach or suggest the limitations of claim 6, namely, that a browser cache is password protected. Hence, at least claim 6 is believed distinguished from the cited references.

II. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 7.22.04

Respectfully submitted,



Patrick C. R. Holmes
Reg. No. 46,380
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorney for Applicants